APPENDIX J

INFORMATION TECHNOLOGY MANAGEMENT GOALS

Section 5123 of the Clinger-Cohen Act requires that the Department establish goals for improving the efficiency and effectiveness of agency operations through the use of information technology (IT) and prepare an annual report, to be included in the budget submission to Congress, on the progress in achieving the goals. This is the Department's fourth Section 5123 annual report.

DOD INFORMATION MANAGEMENT GOALS

Consistent with the Act, the DoD Chief Information Officer (CIO) has published a DoD Information Management (IM) Strategic Plan that focuses on attaining the Department's information superiority goals as well as those of the Act. This will be achieved through global, affordable, and timely access to reliable and secure information for worldwide decision making and operations. To realize this vision, the Department has established the goals described in Table J-1.

Table J-1

DoD Information Management Goals

Goal 1–Become a mission partner:
Identify mission needs and align IT.
Forge effective partnership relationships with customers.
Move toward an information marketplace.
Goal 2–Provide services that satisfy customer information needs:
Build an infrastructure based on architectures and performance.
Ensure DoD systems meet the Year 2000 (Y2K) challenge.
Modernize and integrate the Defense Information Infrastructure, evolving it to the Global Information Grid (GIG).
Introduce new paradigms.
Improve IT management tools.
Goal 3–Reform information technology management processes to increase efficiency and mission contribution:
Institutionalize Clinger-Cohen Act and provisions of Section 8121(b) of the FY2000 DoD Appropriation Act.
Institute fundamental IT management reform efforts.
Promote the development of an IT management knowledge-based workforce within DoD.
Provide the IM/IT support required to ensure individuals with disabilities have equal access to the information environments and opportunities in DoD

Table J-1

DoD Information Management Goals (Continued)

Goal 4–Ensure DoD's vital information resources are secure and protected:
Make Information Assurance (IA) an integral part of DoD mission readiness criteria.
Enhance DoD personnel IA awareness and capabilities.
Enhance DoD IA operational capabilities.
Establish an integrated DoD security management infrastructure.

DOD INFORMATION MANAGEMENT GOALS—ACCOMPLISHMENTS

GOAL 1–BECOME A MISSION PARTNER

The DoD CIO Executive Board continues to be the Department's principal forum to advise the Secretary and Deputy Secretary on the full range of matters pertaining to Subdivision E of the Clinger-Cohen Act. Chaired by the DoD CIO and comprised of DoD Component CIOs, as well as senior managers from the Joint Staff, intelligence, financial, acquisition, and other functional communities, the Board provides a forum for discussing and resolving key information management issues. During the first nine months of its existence, the Board has approved several policies to improve the acquisition, management and use of information and the technology that supports it. These policies address information assurance, telecommunications, network management and operations, architectures, interoperability, computing, software applications, and the overall management of information.

In August, 2000 the DoD CIO convened a three day Worldwide DoD CIO Conference which brought together the key players in the DoD CIO community. Attendees included the CIOs of all of the combatant commands, Services, the Joint Staff, Office of the Secretary of Defense and numerous Defense Agencies, as well as key managers in the mission and functional communities. In addition to panel discussions, executive seminars and roundtable discussions on a wide variety of critical DoD CIO initiatives, emphasis was placed on explicitly defining the roles, responsibilities, and relationships of the CIO within the DoD organization. The intent is to create a greater focus of leadership for information management and a means of coordinating information management and technology activities across the enterprise and with business partners and customers.

GOAL 2—PROVIDE SERVICES THAT SATISFY CUSTOMER INFORMATION NEEDS

The DoD CIO responded to Section 8121(a) of the FY 2000 Defense Appropriations Act by ensuring central registration of all DoD mission critical and mission essential IT systems by March 31, 2000. This automated central registry, while proving useful in its own right, is being expanded to provide for an "integrated management view of DoD IT investments." DoD-wide concerns regarding Information Assurance, Software, Acquisition Oversight, Global Information Grid (GIG), and Enterprise Licensing will all be addressed through data elements gained through future registration updates.

The GIG concept was formulated to enable Full Spectrum Dominance for Joint Vision 2010 and beyond. It envisions a baseline capability integrating all DoD command, control, communications, computers, intelligence, surveillance, and reconnaissance requirements—strategic, operational, tactical, and base/post/camp/station/ship—providing flexible, assured bandwidth to warfighters regardless of environment. The GIG encompasses IT and National Security Systems as defined in the Clinger-Cohen Act.

The DoD CIO initiated work on the GIG, which is the next major increment of the Department's Information Technology Architecture (ITA) as required by Clinger-Cohen. The GIG Architecture effort provides the operational and systems views to complement the already exiting technical view embodied in the Joint Technical Architecture. The GIG product set includes baselines and objectives for full integration of all Joint Mission Areas.

The Defense Management Council approved on September 24, 1999, the overall smart card policy and procedural concepts and directed all DoD components to take actions necessary to implement the use of a standard DoD smart card. This card, which will become the Department’s common access card, will embrace the functions of personnel identification (ID), physical security access, and computer network access. The common access card will be the standard ID card for military personnel (to include the Selected Reserve) and DoD civilian employees.

GOAL 3—REFORM INFORMATION TECHNOLOGY MANAGEMENT PROCESSES TO INCREASE EFFICIENCY AND MISSION CONTRIBUTION

The DoD CIO is a member of the Defense Acquisition Board, thus ensuring that the CIO position is heard on all acquisition deliberations.

The DoD CIO issued a policy memorandum implementing Section 8121(b) of the FY 2000 DoD Appropriation Act, requiring DoD CIO to certify that Major Automated Information Systems (MAIS) are being developed in accordance with the Clinger-Cohen Act. The legislation requires the DoD CIO to notify the Congress of MAIS certifications in a timely manner. To date, five MAIS programs have been certified to Congress as Clinger-Cohen Act compliant.

The Clinger-Cohen Act and other reform legislation require that DoD implement a process whereby IT investments are managed and evaluated based on specific, measurable contributions to DoD mission goals and priorities. To achieve this, the Department has initiated a Families-of-Systems (FoS) approach to managing and overseeing its IT investments in mission areas. Under this approach, mission areas will be analyzed and investments will be grouped by mission capability to establish FoS portfolios. Trade-offs among investments will be made to the optimum benefit of the mission, and benefits will be measured and evaluated in the context of their contribution to the overall success of the mission.

The Enterprise Software Initiative (ESI) is a project that is saving money on commercial-off-the-shelf software by developing a DoD-wide business process for purchasing, distributing, and managing software and creating DoD-wide software agreements. Savings for software licenses and maintenance range from 2 percent to 98 percent off GSA Federal Supply Schedule pricing, depending on the company and number of licenses purchased. DoD savings attributed to ESI increased ten-fold during the past year, due to central financing for software and acceptance of the project. To increase the benefits of ESI, the DoD CIO issued a policy that requires DoD buyers to purchase software from ESI software inventory when available. Buyers must also consider ESI software agreements before they can purchase software from other sources.

In the past year, the Department has been active in a number of internal and external initiatives to employ new and innovative approaches regarding the recruitment, retention, and training of information technology professionals. Following are highlights of key initiatives.

A Deputy Secretary of Defense memorandum dated July 14, 2000, approved implementation of recommendations resulting from an in-depth study of Information Assurance (IA) and Information Technology (IT) recruiting, retention, and training practices within DoD. The implementation of the initiatives will improve the management

of the Department's IA/IT workforce, enabling the Department to: (1) identify and track IA/IT professionals by definitive skill sets, and (2) ensure critical IA/IT management training is completed by individuals in key positions.

The Department is currently working on a variety of initiatives with the Office of Personnel Management to improve the recruitment and retention of IT professionals. These initiatives entail:

- Establishment of new Federal classification standards for the computer specialist series with specialty categories so organizations can readily identify and track critical skill sets. The standards are currently in draft and will be finalized and made mandatory during 2001.

- Participation in studies and reviews of the IT workforce pay structure to develop recommendations regarding specialty pay for select IT skills in the Federal government.

- Revamping of the recruiting/hiring process by improving the solicitation, rating, and interview process. The proposed new recruiting processes are currently being piloted within the Department and other Federal agencies to assist OPM in determining if changes are required prior to full implementation.

The Department chaired a Federal CIO committee consisting of 23 civilian agencies to update the Clinger-Cohen competencies to reflect new and emerging critical information technology management (ITM) requirements. The revised competencies were approved September 2000, by the Federal CIO Council for use as a baseline in determining critical ITM skills, knowledge, training, and workforce requirements of Government officials performing ITM responsibilities.

The Information Resources Management College (IRMC) has been designated as the Department's flagship for information technology management training for senior managers. In addition to the two primary programs offered, the Advanced Management Program and the DoD CIO Certificate Program, the IRMC has established the Information Security/Assurance Certificate Program. This new program has been certified by the National Security Telecommunications and Information Systems Security (NSTISS) Committee as being compliant with the Information Systems Security Professionals standard (NSTISSI No. 4011). The IRM College is one of only four schools nationally that has been certified as meeting the specified NSTISSI training criteria. The National Security Agency also recognized the College's work in this area and awarded the IRMC a three-year appointment as a National Center of Academic Excellence in Information Assurance, for meeting educational requirements of Presidential Decision Directive 63, "Critical Infrastructure Protection".

GOAL 4–ENSURE DOD'S VITAL INFORMATION RESOURCES ARE SECURE AND PROTECTED

Through a Web security initiative, a continued level of scrutiny was applied to the type of information being posted to DoD Web sites.

The Defense Computer Forensics Laboratory continues to develop the skills needed in the future to investigate computer intrusions.

The Department updated its policy on Public Key Infrastructure. This policy sets a milestone of October 2002 by which all DoD active military, civilian, and selected Reserve personnel will have Common Access Card (smart card) tokens hosting their PKI certificates.

In support of Critical Infrastructure (PDD-63) and DoD critical asset protection, the Department conducted a "Table-Top" exercise with the US and UK addressing critical (national) infrastructure protection (CIP/CNIP) problems, with a special interest in those problems rooted in the ongoing highly dynamic revolution in information technology.

The Joint Counterintelligence Evaluation Office continues to ensure that the senior DoD leadership is informed of significant counterintelligence investigative activity. Significant activity includes foreign intelligence threats to DoD critical technologies, information infrastructure, U.S. military operations, and personnel.

We are reengineering the GIG in a manner that will provide, in conjunction with other actions, the "Defense-in-Depth" necessary to protect DoD information systems. The GIG Information Assurance Policy, addresses not only the confidentiality requirement of DoD's information but also its availability, integrity, and the need for strong identification and non-repudiation services.

In response to increasing cyber attacks, DoD accomplished the following:

- During the Melissa Virus incident in March 2000, the maturing role of the Joint Task Force-Computer Network Defense (JTF-CND) became evident. In cooperation with the DOD Computer Emergency Response Team (CERT) and the JTF's service components, the JTF-CND was able to quickly assess the threat, develop a defensive strategy, and direct appropriate defensive actions. Again in May 2000, the LOVELETTER virus provided another example of JTF-CND rapid action. The JTF staff rapidly identified the potential damage and provided rapid notification to the CINCs, Services, and agencies, which enabled them to effectively respond.

- In 1999, DISA established an Information Assurance Vulnerability Alert (IAVA) system for distributing vulnerability information to all DoD elements on behalf of OSD. So far this year DISA has issued, 3 IAVAs (alerts), 6 IAVBs (bulletins) and 11 technical advisories. DISA also developed a database to immediately distribute vulnerability information to each system administrator and to track and report on their response to these alerts.

- Improved its ability to analyze data and assess attacks.

- Conducted red team exercises to improve operational readiness and continued improvements to the red team methodology.

CONCLUSION

By aggressively pursuing a well-articulated set of DoD CIO priorities, DoD has:

- Established the DoD CIO Executive Board as a decision making forum that is actively reviewing and approving policies which are designed to enhance compliance with the Clinger-Cohen Act.

- Clearly established criteria and policy that creates a focus of leadership for the DoD CIO.

- Established the Global Information Grid with objectives toward full integration of all Joint Mission Areas.

- Initiated the Family-of-Systems Management and Oversight process.
- Continued significant improve in Information Systems Security.

Accomplishment of these steps has enabled the Department to move forward toward more complete implementation of the Clinger-Cohen Act of 1996.